Vysoká škola báňská – Technická univerzita Ostrava

Fakulta bezpečnostního inženýrství

Katedra bezpečnostního managementu

Ochrana osobních údajů a informací městského úřadu

Student: Veronika Kulová
Vedoucí bakalářské práce: Ing. Václav Veselý

Studijní obor: Technická bezpečnost osob a majetku
Datum zadání bakalářské práce: 28. 11. 2008
Termín odevzdání bakalářské práce: 30. 4. 2009

VŠB - Technická univerzita Ostrava
Fakulta bezpečnostního inženýrství
Katedra bezpečnostního managementu

Akademický rok 2008/2009

Zadání bakalářské práce

Student: **Veronika Kulová**

Studijní program: B3908 Požární ochrana a průmyslová bezpečnost

Studijní obor: 3908R005 Technická bezpečnost osob a majetku

Téma: Ochrana osobních údajů a informací městského úřadu
The Protection of Personal Data and Information at a Municipal Office

Zásady pro vypracování:

Cíl práce:
Zjistit a popsat aktuální rizika spojená s ochranou osobních údajů a informací v budově městského úřadu a na základě teoretických znalostí navrhnout optimální způsob pro jejich ochranu v tomto objektu.
Charakteristika práce:
Popis zadané problematiky, základní východiska, právní rámec ochrany osobních údajů a informací, současný způsob zajištění ochrany osobních údajů a informací u městských úřadů, srovnání způsobů ochrany osobních údajů a informací u nás a v zahraničí, návrh optimálního způsobu ochrany osobních údajů a informací městského úřadu.

Seznam doporučené odborné literatury:

Zákon č. 140/1961 Sb. ve znění pozdějších předpisů
Zákon č. 141/1961 Sb. ve znění pozdějších předpisů
Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých údajů
Toms, L., Koníček, T., Kocábek, P.: Zabezpečení dveří a oken - rizikových míst objektů, MV ČR, odbor prevence kriminality, Praha, 1997
Brabec, F. a kol.: Bezpečnost pro firmu, úřad, občana, Public History, Praha, 2001
ČSN P ENV 1627 Okna, dveře, uzávěry - odolnosti proti násilnému vniknutí. Požadavky a klasifikace, 2000, Český normalizační institut.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Václav Veselý**

Datum zadání: 28.11.2008

Datum odevzdání: 30.04.2009

doc. RNDr. Jiří Švec, CSc.
vedoucí katedry

doc. Dr. Ing. Aleš Dudáček
děkan fakulty

Místopřísežné prohlášení:

Místopřísežně prohlašuji, že jsem celou bakalářskou práci vypracovala samostatně.

V Ostravě dne 30. dubna 2009 _____

Veronika Kulová

Poděkování:

Ráda bych poděkovala vedoucímu bakalářské práce Ing. Václavu Veselému za ochotu, cenné rady, odborné vedení, připomínky a značnou podporu při zpracování dané problematiky.

Anotace

KULOVÁ, Veronika. *Ochrana osobních údajů a informací městského úřadu*. Ostrava, 2009. 44 s. VŠB-Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství. Vedoucí bakalářské práce Ing. Václav Veselý.

Bakalářská práce je věnována problematice ochrany osobních údajů a informací na městském úřadě. Je zde provedena analýza rizik osobních údajů a informací. Tyto rizika jsou identifikovány a vyhodnocovány pomocí Ishikawova diagramu, FTA a metody FMEA. Z výsledků je navrženo řešení zabezpečení informací k zmírnění těchto rizik. Práce přináší přehled o možných způsobech ochrany informací v organizacích.

Klíčová slova: Osobní údaj, informace, analýza, ochrana informací

Annotation

KULOVÁ, Veronika. *The Protection of Personal Data and Information at a Municipal Office* Ostrava, 2009. 44 pgs.. VŠB-Technical university of Ostrava, Faculty of Safety Engineering, Leader of bachelor works Ing. Václav Veselý.

This bachelor work is aimed at the problems the protection of personal data and information at a municipal offic. Is here effected risk analysis and jeopardy of personal data and information. These risks are identified and evaluated according to. These risks are identified and evaluated through Ishikaw diagram, FTA and Metod FMEA. For record is chosen security information to modulation these risks. This work includes summary of methods for the protection of information in organizations.

Keywords: personal data, information, analysis, the protection of information

Obsah

Úvod

Ochrana informací a osobních údajů je novým právním a společenským problémem. Před lety se pro práci s informacemi všeho druhu používaly běžné psací potřeby a klasické ruční evidenční prostředky. Zlom nastal se zavedením výpočetní techniky, zejména osobních počítačů a informačních technologií do administrativy. Současná společnost stále častěji využívá informační systémy a technologie v nejrůznějších oblastech lidské činnosti. Dalo by se říct, že společnost jednadvacátého století bude zcela postavena na informačních technologiích. Zájem institucí o naše osobní údaje a náš zájem nebo nezájem o jejich ochranu patří k aktuálním tématům ve veřejném životě obyvatel České republiky. S tím jsou spojena nová rizika při zpracování a uchovávání informací nejrůznějšího druhu. Městský úřad, jako orgán územní samosprávy, zpracovává velké množství informací a osobních údajů, proto je nezbytné aby tyto informace byli dostatečně zabezpečeny. Hlavním cílem ochrany osobních údajů není absolutně bránit v používání osobních údajů jiných osob, ale zabránit zneužití či zničení těchto údajů. [5]

Cílem této práce je analýza aktuálních rizik spojených s ochranou osobních údajů a informací v budově městského úřadu a na základě teoretických znalostí navrhnout optimální způsob pro jejich ochranu v tomto objektu.

1 Právní úprava a technické normy

Jedním z hlavních důvodů, proč dochází k realizaci zabezpečení osobních údajů a informací, jsou povinnosti vyplývající z platných zákonů a vyhlášek. V České republice není zákon, který by řešil zabezpečení informací komplexně. Přesto existuje mnoho zákonů a vyhlášek, které se k problematice bezpečnosti informací vztahují. [6]

1.1 Ústava České republiky

Zákon č. 1/1993 Sb., Ústava České republiky (dále jen Ústava ČR), ve znění pozdějších předpisů. Ústava ČR je souhrn právních norem deklarující základní práva občanů a definující demokratické principy České republiky jako svrchovaného, jednotného a výkonného demokratického státu. Text Ústavy ČR je rozdělen do preambule a osmi hlav:

- Základní ustanovení
- Moc zákonodárná
- Moc výkonná
- Moc soudní
- Nejvyšší kontrolní úřad
- Česká národní banka
- Územní samospráva
- Přechodná a závěrečná ustanovení

1.2 Listina základních práv a svobod

Listina základních práv a svobod (dále jen Listina) je ústavním zákonem č. 2/1993 Sb., o vyhlášení listiny základních práv a svobod, ve znění pozdějších předpisů. Definuje práva a svobody v Listině uvedené jako nezadatelné, nezcizitelné, nepromlčitelné a nezrušitelné.
Listina deklaruje mimo jiné nedotknutelnost osoby a jejího soukromí, osobní svobodu, právo k zachování lidské důstojnosti, osobní cti, dobré pověsti a ochrany jména. Dále pak definuje problematiku ochrany soukromého, osobního života a právo na ochranu před neoprávněným shromaždováním, zveřejňováním nebo jiným zneužíváním údajů o osobách, čímž se zabývají články 10, 13 a 17.

V článku 10 je chráněna lidská důstojnost, jeho dobrá pověst, osobní čest, jméno a soukromí. Přestože se v tomto článku přímo výraz informace nevyskytuje, nýbrž výraz „údaje o své osobě“, jsou tyto informace osobními údaji, neboť se vztahují k určité osobě.

V článku 13 je uvedeno, že „nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů“ bez ohledu na to, jestli jsou uchovávány nebo přenášeny jakýmikoliv způsoby. Tento zákaz se týká jak fyzických osob, právnických osob tak i státu, a současně platí jak pro uchovávané, tak pro přenášené informace.

K informacím se dále váže článek 17 v druhém oddílu, který se zabývá především politickými právy, jako je právo svobodného projevu, právo vlastního názoru, zákaz cenzury či právo na informace. Zároveň je však ve čtvrtém odstavci tohoto článku stanoveno, že onu svobodu „lze omezit zákonem, jde-li o opatření v demokratické společnosti nezbytná pro ochranu práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost, ochranu veřejného zdraví a mravnosti“. Dále jsou v pátém odstavci stanoveny povinnosti státních orgánů a orgánů územní samosprávy „poskytovat informace o své činnosti“, přičemž zákon stanoví podmínky a provedení.

1.3 Trestní zákon

Zákon č. 140/1961 Sb., trestní zákon (dále jen trestní zákon), ve znění pozdějších předpisů. Trestní zákon chrání zájmy společnosti, ústavní zřízení České republiky, práva a oprávněné zájmy fyzických a právnických osob. Stanovuje skutkové podstaty trestných činů.

1.4 Zákon o trestním řízení soudním

Zákon č. 141/1961 Sb., zákon o trestním řízení soudním, ve znění pozdějších předpisů. Upravuje postup orgánů činných v trestním řízení tak, aby trestné činy byly náležitě zjištěny a jejich pachatelé podle zákona spravedlivě potrestáni. Trestní řízení musí upevňovat zákonnosti, předcházet a zamezovat trestné činnosti, vychovávat občany v duchu důsledného zachovávání zákonů a pravidel občanského soužití i čestného plnění povinností ke státu a společnosti. Každý občan má právo a povinnost pomáhat při dosahování účelů trestního řízení.

1.5 Zákon o ochraně osobních údajů

Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, je uplatňován v organizacích všeho druhu. V našem případě hraje klíčovou roli, protože upravuje zásady zpracování osobních údajů v informačních systémech, a to nejen v systémech automatizovaných, ale také v systémech, které výpočetní techniku nevyužívají. Musí se jím řídit státní orgány, orgány územní samosprávy, orgány veřejné moci, fyzické a právnické

osoby, které zpracovávají nebo jinak nakládají s osobními údaji. Rozumí se tím zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace osobních údajů. Smyslem zákona o ochraně osobních údajů je zaručení práva na ochranu občana před neoprávněným zasahováním do jeho soukromého a osobního života a neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním osobních údajů dané Listinou základních práv a svobod. Vlivem rozvoje informačních technologií je toto právo stále více narušováno. Zákon se nevztahuje na zpracování osobních údajů, které provádí fyzická osoba výhradně pro osobní potřebu a na nahodilé shromažďování osobních údajů, pokud tyto údaje nejsou dále zpracovávány.

Osobní údaj je definován jako jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů je určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.

Citlivý údaj je osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů. Citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů.

Subjekt osobních údajů (dále jen subjekt) je fyzická osoba, k níž se osobní údaje vztahují.

Správcem osobních údajů (dále jen správce) je každý subjekt, který určuje proč k zpracování dochází a prostředky jimiž jsou osobní údaje zpracovány, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele.

Zpracovatel osobních údajů je každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje. Má stejné povinnosti jako správce.

Povinnosti správce při zpracování osobních údajů

Povinnosti správce zakotvuje zákon o ochraně osobních údajů především v § 5, 6, 9, 10, 11, 12, 13, 16, 19, 20, 21 a 27. Jedna z hlavních povinností správce je stanovit účel, pro něž mají být osobní údaje zpracovány, formulované v § 5 odst. 1 písm. a). Další povinností je určit prostředky a způsob zpracování osobních údajů, tak jak ji ukládá § 5 odst. 1 písm. b). Správce musí zjistit, zda se zpracování týká oznamovací povinnosti podle §16, který stanovuje, že kdo hodlá zpracovávat osobní údaje, je povinen tuto skutečnost oznámit Úřadu pro ochranu osobních údajů. Toto oznámení musí být učiněno písemně.

Dříve, než správce začne osobní údaje zpracovávat, musí zjistit, zda se ho netýká povinnost získat souhlas subjektu údajů (dále jen souhlas). Zákon o ochraně osobních údajů stanovuje podmínky souhlasu v § 5 odst. 2 a 4 a v § 9 písm. a). V odst. 2 je uveden výčet podmínek, při jejichž naplnění správce nemusí získat souhlas. Podle § 10 má správce povinnost dbát, aby subjekt údajů neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a dbát na ochranu před neoprávněným zasahování do soukromého a osobního života subjektu údajů. V § 11 správce musí posoudit, v jaké míře má vůči subjektu údajů informační povinnost. Zjednodušeně subjekt údajů má vždy právo na informace o shromažďování osobních údajích, o správci , k jakému účelu a jak dlouho budou zpracovávány a komu budou předávány. Výjimku z povinnosti poskytovat informace je ustanoveno v § 11 odst. 3.

Dále musí zpracovávat pouze přesné osobní údaje, které získal v souladu s tímto zákonem. Je-li to nezbytné, osobní údaje aktualizuje. Uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování, shromažďovat osobní údaje pouze otevřeně, nesdružovat osobní údaje, které byly získány k rozdílným účelům. Poskytování osobních údajů do zahraničí upravuje § 27 tohoto zákona a stanovuje podmínky, jež jsou nutné splnit, aby mohly být osobní údaje poskytnuty do zahraničí a nebyl přitom porušen zákon.

Pro tuto práci je nejdůležitější povinnost správce přijmout bezpečnostní opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost je zakotvená v § 13.

Povinnosti správce při ukončení zpracování

V případě, že osobní údaje už nejsou zpracovávány, ale jsou dále uchovávány, tak stále trvá povinnost přijmout bezpečnostní opatření. Jestliže se správce chystá ukončit zpracování osobních údajů, je jeho povinností oznámit tuto skutečnost ÚOOÚ a neprodleně

udat způsob, jakým naložil s osobními údaji. V ustanovení § 20 je uvedeno, že správce je povinen provést likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovány. Při likvidaci osobních údajů se myslí fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování.

Povinnosti zaměstnanců správce

Je nutné, aby povinnostmi byly zatíženy i konkrétní fyzické osoby, které tyto údaje zpracovávají. V § 14 je uvedeno, že zaměstnanci správce, kteří zpracovávají osobní údaje na základě smlouvy se správcem, mohou zpracovávat osobní údaje pouze za podmínek a v rozsahu stanoveném správcem. Dále je § 15 stanovena nezbytnost zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatření.

Přístup k osobním údajům

Pokud subjekt údajů požádá o informace o zpracování svých osobních údajů, je správce povinen tyto informace bez zbytečného odkladu předat.

Úřad pro ochranu osobních údajů (dále jen ÚOOÚ) je nezávislým orgánem, který:

- Provádí dozor nad dodržováním zákonem stanovených povinností při zpracování osobních údajů,
- Vede registr povolených zpracování osobních údajů,
- Přijímá podněty a stížnosti občanů na porušení zákona,
- Poskytuje konzultace v oblasti ochrany osobních údajů. [12]

1.6 Technické normy v oblasti zabezpečení objektu a informačních systémů

Pro správné zabezpečení informací musíme vycházet ze závazných technických norem. Ty řeší rozdělení a požadavky na prostředky zabezpečovacích systémů.

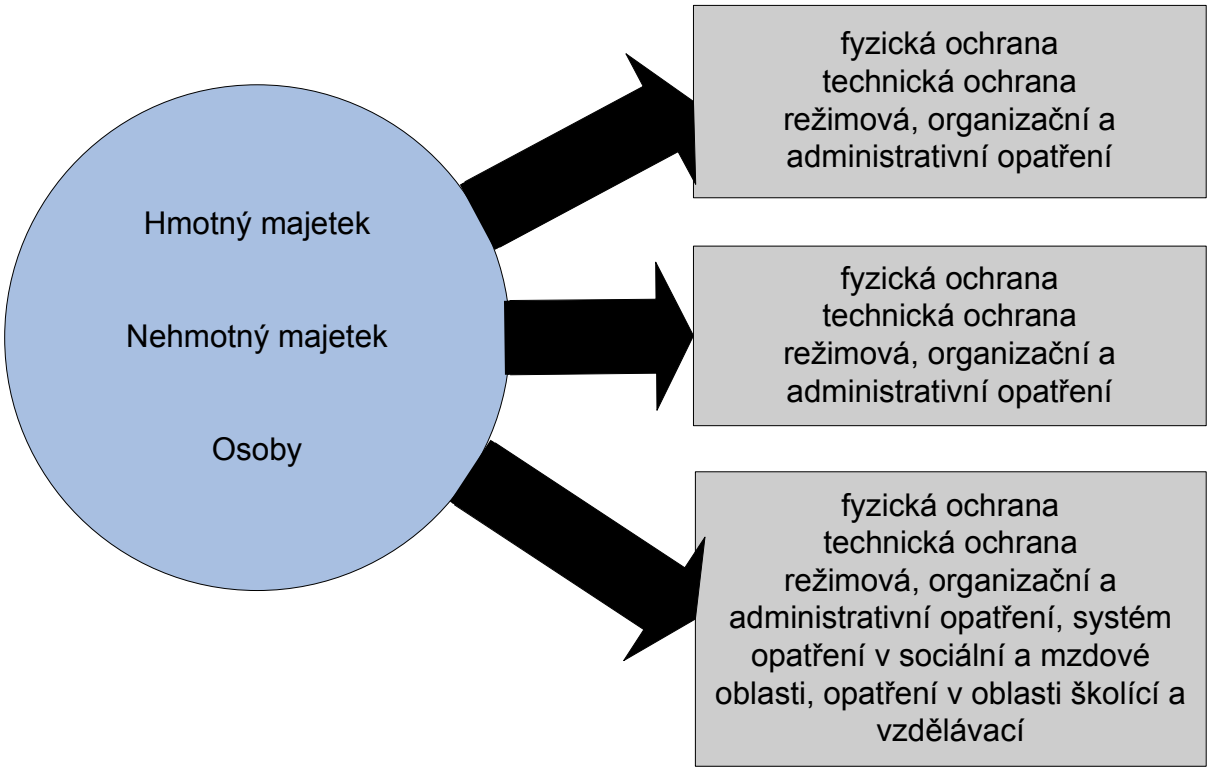
- ČSN P ENV 1627 Okna, dveře, uzávěry - Odolnost proti násilnému vniknutí. Požadavky a klasifikace,

- ČSN EN 1143-1 Bezpečnostní úschovné objekty – Požadavky, klasifikace a metody zkoušení odolnosti proti vloupání. Část 1: Skříňové trezory, trezorové dveře a komorové trezory,
- ČSN EN řady 50133 Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích,
- ČSN 91 6012 Bezpečnostní úschovné objekty - Požadavky, klasifikace a metody zkoušení odolnosti proti vloupání. Trezory se základní bezpečností,
- ČSN EN 1300 Bezpečnostní úschovné objekty - Klasifikace zámků s vysokou bezpečností vzhledem k jejich odolnosti proti nepovolenému otevření,
- ČSN EN řady 50130 Poplachové systémy – Všeobecně,
- ČSN EN 50131-1 Poplachové systémy – Elektrické zabezpečovací systémy uvnitř a vně budov. Část 1: Všeobecné požadavky,
- ČSN EN řady 50132 Poplachové systémy - CCTV sledovací systémy pro použití v bezpečnostních aplikacích,
- ČSN EN řady 50133 Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích,
- ISO/IEC 177799:2005 (ISO/IEC 27002) Soubor postupů pro management bezpečnosti informací,
- ISO/IEC 27001:2005 Systémy managementu bezpečnosti informací – Požadavky,
- ČSN ISO/IEC TR 13335-1:2004 Směrnice pro řízení bezpečnosti IT – Část 1: Pojetí a modely bezpečnosti IT,
- ČSN ISO/IEC TR 13335-2:2004 Směrnice pro řízení bezpečnosti IT – Část 2: Řízení a plánování bezpečnosti IT,
- ČSN ISO/IEC TR 13335-3:2004 Směrnice pro řízení bezpečnosti IT – Část 3: Techniky pro řízení IT,
- ČSN ISO/IEC TR 13335-4:2004 Směrnice pro řízení bezpečnosti IT – Část 4: Výběr ochranných opatření.

2 Teorie zabezpečení objektu

V dnešní době technických vymožeností se ochrana majetku řeší v podstatě stejně jako před staletími. Kamenné hradby, vodní příkopy, padací mosty, mříže, kované truhlice zabraňovaly poškození nejen válkami, ale chránily také před zloději. Elektrická zabezpečovací signalizace s kamerovými systémy nahradila hlídky a strážní věže, organizační a režimová opatření nahradily rozkazy velitele, identifikační karty nahradily různé pečetě a talismany.

Předmětem zájmu bezpečnosti je ochrana hmotného majetku, nehmotného majetku a osob. Při komplexním zabezpečení objektu musí být bezpečnostní systém navržen tak, aby jeho jednotlivé prvky poskytovali požadovaný stupeň bezpečnosti, jak je uvedeno na Obrázku 1. Obecně platí, že ochrana je tak silná, jako její nejslabší článek. [2,7]



Obrázek 1: Komplexní bezpečnost organizace

2.1 Fyzická ochrana

Fyzická ochrana je nejpoužívanější způsob ochrany majetku a osob. Jako jediná je schopna provést v případě nutnosti zásah k odvrácení hrozícího nebo trvajícího nebezpečí. Pokud chceme, aby bylo použití technických prostředků ochrany (zejména elektronických zabezpečovacích a signalizačních systémů, kamerových systémů apod.) efektivní, je třeba je doplnit fyzickou ochranou. Pokud budeme mít nejnovější kamerový systém s nejlepší dostupnou technologií, ale nebudeme mít nikoho, kdo by snímaný prostor na monitorech sledoval, bude nám tento systém k ničemu. Fyzickou ochranu – hlídací službu – lze realizovat prostřednictvím soukromé bezpečnostní služby, vlastní ochrannou službou organizace a Policií České Republiky.

Fyzická ochrana obsahuje:

- Ochranu a ostrahu majetku na místech veřejnosti nepřístupných
- Ochranu a ostrahu majetku na místech veřejnosti přístupných
- Ochranu a ostrahu majetku na místech určených pro styk se zákazníkem
- Ochranu a ostrahu při transportu peněz, cenností a zbraní
- Osobní ochranu osob
- Zajištění pořádku v místech pořádání veřejných shromáždění, slavností, sportovních podniků, kulturních akcí apod.
- Zajištění výjezdu zásahové skupiny při poplachu prostřednictvím pultu centralizované ochrany

Formy fyzické ochrany:

Strážní služba

Při strážní službě pracovník fyzické ochrany zabezpečuje většinou obvodovou ochranu majetku. Hlavně pozoruje objekt a okolí včetně přilehlých komunikací a parkovišť, zabraňuje nedovelené činnosti směřující k narušení objektu, prostoru či osobě apod. Může být realizována na pevných strážních stanovištích nebo jako pochůzková (hlídková) služba.

Bezpečnostní dohled

Zpravidla je realizován uvnitř chráněného objektu či prostoru. Buď jako celoplošný dohled nebo jako dohled nad určitým prostorem, místem, budovou, osobou apod. Hlavně

sleduje oprávněný pohyb a činnost osob, dodržování stanoveného vnitřního režimu, doprovází osoby a dohlíží nad činnostmi a pracemi prováděnými cizími pracovníky apod.

Bezpečnostní ochranný doprovod

Jde o bezpečnostní ochranný doprovod osob, peněžních hotovostí a cenností, kamionové přepravy, přepravy po železnici, lodní přepravy, letecké přepravy a dalších způsobů dopravy a přesunů. Spíše než fyzické ochraně se blíží detektivní službě, proto by bezpečnostní ochranný doprovod měl být v každém případě záležitostí speciálně vycvičených a vyškolených pracovníků soukromé bezpečnostní služby. Ochranný doprovod může být realizován pěším způsobem, ve vozidle, ve kterém je náklad přepravován, doprovodným vozidlem nebo kombinovanými způsoby.

Bezpečnostní průzkum

Slouží k prohlídce prostředí, ve kterém není zajištěna trvalá ochrana, ale jde spíše o momentální zjištění a upřesnění stavu veřejného pořádku, bezpečnosti majetku a osob v určitém čase a prostoru. Bezpečnostní průzkum bývá realizován hlídací službou přímo nebo na dálku pomocí elektronických systémů, nebo soukromými detektivy.

Kontrolní propustková služba

Zabraňuje neoprávněnému vstupu osob a vjezdu vozidel, vnášení nebo vynášení předmětů, materiálu, zboží, výrobků, dohlíží a eviduje přicházející a odcházející osoby a přijíždějící a odjíždějící vozidla, poskytuje v potřebném rozsahu informace návštěvám objektu či prostoru, zajišťuje respektovaní stanoveného režimu návštěv, vede knihu příchodů a odchodů zaměstnanců a návštěv, odemyká a uzamyká vchody a vstupy do objektu, eviduje vydávání klíčů od vstupů do objektu a plní další specifické úkoly.

Bezpečnostní zásah

V případě aktivování elektronického zabezpečovacího systému vyjede zásahová skupina na základě informace z pultu centralizované ochrany na místo předpokládaného narušení.

2.2 Technická ochrana

Technický prostředek je bezpečnostní prvek, jehož použitím se zabraňuje, ztěžuje nebo oznamuje narušení ochrany objektu nebo zabezpečené oblasti. Spočívá v zajištění objektu použitím příslušných mechanických, elektronických a elektrických zařízení. Obecně lze technickou ochranu rozlišovat z hlediska prostorového zaměření na perimetrickou (obvodovou), plášťovou, prostorovou a předmětovou.

Obvodová ochrana neboli ochrana perimetru brání narušení obvodu nebo signalizuje narušení obvodu. Obvodem objektu obyčejně rozumíme jeho katastrální hranice realizované obvykle přírodními nebo umělými bariérami na přilehlých pozemcích. Mezi prvky obvodové ochrany patří různé druhy plotů, které jsou znázorněny na Obrázku 2, podhrabové překážky, vstupy, vjezdy. Patří zde také speciální technické, elektronické, popřípadě elektronicko - mechanické venkovní zabezpečovací systémy. Jsou důležitou součástí střežení rozsáhlých komplexů budov a prostorů jako jsou např. elektrorozvodny, letiště, věznice, průmyslové objekty, vodárny apod. Účelem tohoto perimetrického střežení je zachytit případného narušitele technickými prostředky včas, tedy v okamžiku, kdy ještě nepáchá trestnou činnost ve střežených prostorách. Základním požadavkem na prvky venkovní perimetrické ochrany je nezávislost funkce na klimatických podmínkách. V současné době se využívají např. infračervené pasivní detektory, infračervené závory, mikrovlnné závory, mikrofonní nebo optické kabely snímající vibrace, štěrbinové kabely, deformační senzory, tlakové podzemní hadice, videodetektory pohybu apod.

Obrázek 2: Prvky obvodové ochrany

Plášťová ochrana brání narušení pláště objektu nebo signalizuje narušení pláště objektu. Mezi prvky plášťové ochrany patří mříže, bezpečnostní folie, čidla v blízkosti

možného vstupu do objektu, které jsou znázorněny na Obrázku 3, poplachové folie, drátové detektory apod. [13]

Obrázek 3: Prvky plášťové ochrany

Prostorová ochrana spočívá především v signalizaci jevů s charakterem nebezpečí v prostoru bezprostředně obklopujícím chráněné hodnoty a předměty. Mezi prvky prostorové ochrany patří zejména různé druhy čidel, jak je zobrazeno na Obrázku 4 (prostorové PIR čidlo a detektor tříštění skla), odposlechové prostředky, šumové generátory apod.

Obrázek 4: Prvky prostorové ochrany

Předmětová ochrana signalizuje bezprostřední přítomnost pachatele u chráněného předmětu, jak v případě jeho napadení, tak i při neoprávněné manipulaci s tímto předmětem či úschovným místem nebo ztěžuje pachateli dostat se k chráněnému předmětu. Mezi prvky předmětové ochrany patří kapacitní, speciální a tlakové detektory, detektory na obrazy, nášlapné koberce a trezory, které jsou na Obrázku 5.

Obrázek 5: Prvky předmětové ochrany

2.2.1 Mechanické zábranné systémy

Jedná se o nejstarší typ ochrany a spočívá v použití nejrůznějších mechanických zařízení, pomocí kterých můžeme spolehlivě zajistit ochranu určitého objektu, prostoru, místnosti, předmětu apod. Jde o vytvoření různých zábran a bariér, které znemožní odcizení předmětů, zařízení, nebo vytvoření překážek, které pachateli ztíží dosažení jeho cíle. Jejich charakteristickým znakem je jejich bezpečnostní úroveň představována průlomovou odolností. Mezi mechanické zábranné prostředky patří zejména mříže, zámky a bezpečnostní uzamykací systémy, závory, rolety, úschovné objekty, ploty, bezpečnostní dveře, bezpečnostní folie a skla. [10]

2.2.2 Elektrické a elektronické zabezpečovací systémy

Jedná se relativně o nový druh ochrany, její historie se počítá zhruba na 150 let. Její význam prudce stoupá a ze dne na den se objevují nové a lepší zabezpečovací systémy. Nejsou typickým zabezpečovacím prvkem, protože ne vždy tyto systémy plní roli zabezpečení v pravém slova smyslu. Ve většině případů nezabrání pachateli v průniku do objektu, ale jsou určeny k tomu, aby informovaly o možné hrozbě, zpravidla obsluhu, a vyvolali tak reakci, která bude zaměřena na provedení zabezpečovacích opatření. Předávána informace může mít podobu zvukového signálu, obrazového signálu, světelného signálu apod. [11]

Elektrická zabezpečovací signalizace (dále jen EZS)

EZS je soubor zařízení složený z několika částí, tvořících komplexní zabezpečovací řetězec (čidla, ústředny, přenosové prostředky, signalizační a ovládací panely). Propojení čidel s ústřednou může být realizováno tzv. drátově pomocí elektrických kabelů nebo bezdrátově pomocí rádiových vln. EZS monitoruje vstup neoprávněných osob do prostorů, které jsou touto signalizací střeženy, a následně při vyhlášení poplachu dávají podnět k přivolání policie nebo bezpečnostní služby.

Elektrická požární signalizace (dále jen EPS)

Systémy EPS tvoří důležitou součást systémů protipožární ochrany objektů a budov. Elektrická požární signalizace zajišťuje včasnou a rychlou identifikaci a lokalizaci vzniku ohniska požáru. Nasazením systému EPS je tak možné zabránit vzniku velkých materiálových ztrát a v horších případech i ztrátě lidských životů. EPS lze začlenit do integrovaných bezpečnostních a havarijních systémů ochrany majetku, osob. Systém EPS tvoří vyhodnocovací ústředna, různé typy hlásičů, koncová a ovládací zařízení. EPS informuje uživatele o vzniku požáru akustickou a optickou signalizací přímo v objektu nebo pomocí zařízení dálkového přenosu signalizace na stanoviště pultu centrální ochrany (dále jen PCO), který je umístěn u hasičského záchranného sboru (dále jen HZS). Hlásiče EPS pracují na různých fyzikálních principech. Vyhodnocují optické, ionizační nebo teplotní parametry prostředí, ve kterém jsou umístěny. Všechny detektory jsou dnes již vybaveny složitou elektronikou řízenou procesorem, umožňující eliminovat plané poplachy. Systémy EPS mohou být instalovány jako samostatné aplikace nebo jako součásti vyšších integrovaných systémů řízení budov.

Kamerové systémy

Kamerové systémy (dále jen CCTV – Closed Circuit Television) jsou velmi významným prostředkem pro monitorování a to nejen pro bezpečnostní účely, ale také pro sledování různých výrobních procesů v průmyslu apod. Černobílé nebo barevné CCTV systémy tvoří: kamery, monitory, videopřepínače, multiplexery, videomatice, záznamová zařízení, detektory pohybu, přenosové cesty, audio komponenty apod.

Komunikační sítě a prostředky

Aby byl daný bezpečnostní systém funkční, musí být zajištěna ochrana komunikačních prostředků a sítí. Tyto prostředků pracují na principu vzdálené komunikace mezi nejméně dvěma subjekty. Využívají se především při dorozumívaní o vzniku krizové situace, přivolávání posil apod. Nejrozšířenějším komunikačním prostředkem je pevné spojení pomocí klasického telefonního přístroje.

Dále do elektrických a elektronických systémů patří pulty centralizované ochrany, systém kontroly strážní služby, prostředky pro detekci látek, prostředky proti aktivnímu a pasivnímu odposlechu, prostředky k monitorování určeného prostoru, prostředky k ochraně určeného prostoru apod.

2.2.3 Ostatní technické prostředky

Mezi tyto prostředky patří např.:

- prostředky k ochraně před požárem a únikem nebezpečných látek (např. kyslíkové masky, ochranné oděvy, hasící přístroje apod.),
- zbraně k osobní ochraně, nebo prostředky k osobní ochraně před zbraněmi (např. neprůstřelné vesty, helmy apod.),
- k ochraně informací, mohou sloužit zařízení na fyzické ničení nosičů informací (např. šrotovačky),
- prostředky k ochraně uložených dat na PC (např. antivirové programy, kryptografická ochrana),
- apod.

2.3 Režimová ochrana

Režimová ochrana je soubor režimových opatření, které určují, kdo a kdy může vstupovat do objektu, docházka zaměstnanců, kdo zodpovídá za odblokování systému zabezpečovací techniky, kdo a jak kontroluje pohyb cizích osob v objektu, klíčový režim, systémové opatření pro chování v krizových situacích apod. Režimová ochrana v sobě zahrnuje organizační, administrativní a věcná opatření, která směřují k zajištění bezporuchového fungování celého zabezpečovacího systému objektu.

Režimovými opatřeními jsou:

a) režim vstupu a výstupu osob a vjezdu a výjezdu dopravních prostředků,

b) režim pohybu osob, dopravních prostředků v objektu a jeho jednotlivých částech,

c) režim manipulace s klíči, identifikačními prostředky a médii, které se používají pro systémy zabezpečení vstupů, kterým se zejména určuje způsob označování, přidělování a odevzdávání klíčů, jejich úschovy a evidence, uložení duplikátů a způsob jejich použití,

d) režim manipulace s technickými prostředky a jejich používání.

Režimová opatření se týkají :

- činnosti pracovníků uvnitř organizace (vlastních zaměstnanců)
- pohybu a chování osob přicházejících zvenčí včetně oběhu dokladů a informací uvnitř organizace
- vstupy informací, dat, dokumentů vně podniku.

Základní dokumenty režimové ochrany:

- Statut organizace – vyjadřuje cíl a účel činnosti organizace, důležitost jejího postavení.
- Organizační řád organizace – konkretizuje strukturu podniku a vazby jednotlivých částí i vlastní provozní činnosti. Obsahuje i ustanovení týkající se ochrany organizace.
- Pracovní řád – rozvádí funkční náplně jednotlivých kategorií pracovníků, jejich práva a povinnosti, eventuelně pracovní postupy. Obsahuje podrobně zpracovanou komplexní ochranu včetně ochrany dat a informací. Musí se stanovit i stupeň utajení jednotlivých funkcí.
- Spisový řád – stanoví zásady oběhu dokumentů, systém jejich posuzování a schvalování včetně další činnosti jejich předávání (kopírování, ukládání, poštovní přeprava, postupy v případě ztráty apod.). S tím souvisí i manipulace a režim dalších administrativních pomůcek, jako razítka, kopírovací papíry, barvící pásky, magnetická media apod.
- Skartační činnost – vytříďování spisů podle skartačního řádu, který stanovuje skartační lhůty, způsob vytříďování agendy, určování jejich důležitosti a způsob likvidace.

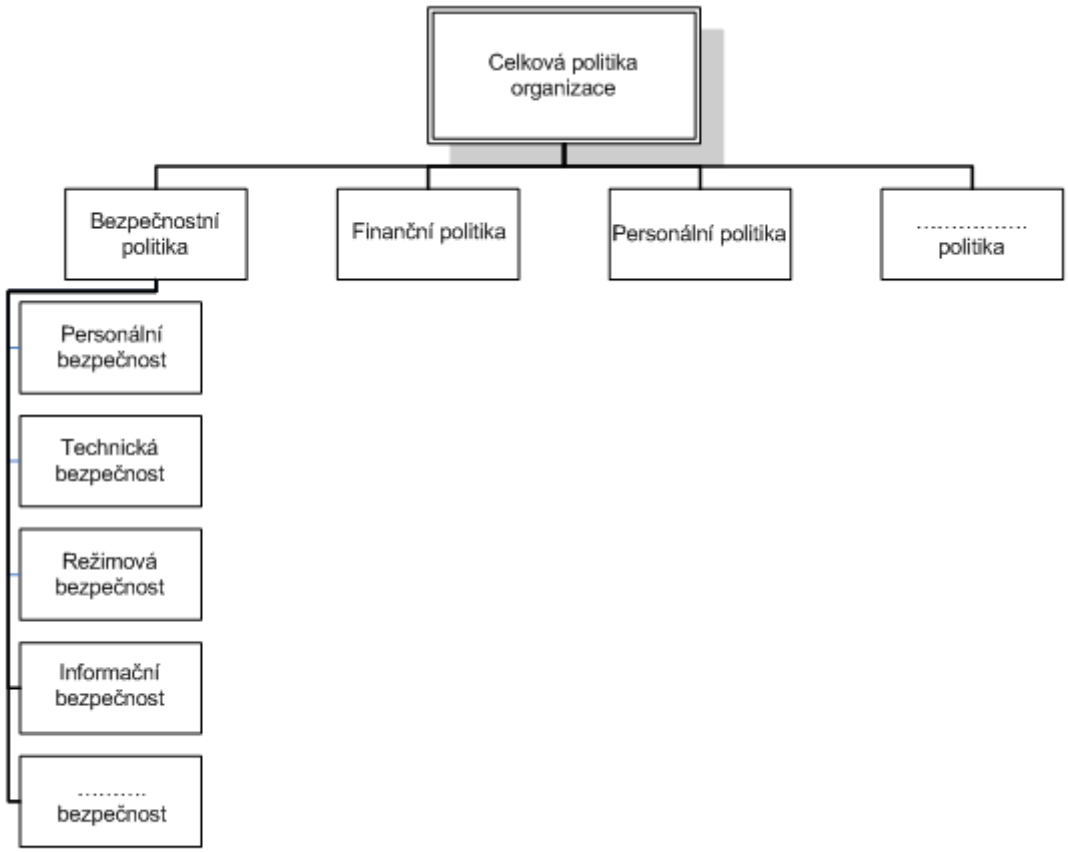
2.4 Bezpečnostní politika organizace

Bezpečnostní politika organizace je soubor odpovědí top managementu organizace především na tři základní otázky:

- co má organizace v oblasti bezpečnosti činit a proč,
- jakých cílů v oblasti bezpečnosti chce dosáhnout,
- jaká opatření přijmout, aby stanovených cílů bylo dosaženo.

Aby byla bezpečnostní politika účelná a stala se účinným nástrojem k prosazení bezpečnostních opatření a zásad v ní obsažených, měla by být vyjádřena v písemné formě. Dokument bezpečnostní politiky zahrnuje celkovou bezpečnost organizace a má velmi obecný charakter. Bezpečnostní politika je podřízena celkové politice organizace a může se stát, že se s ní dostane do střetu. Jeden z nejčastějších důvodů je, že ekonomické cíle organizace a bezpečnostní cíle organizace nebývají zcela totožné.

Problematika bezpečnosti organizace je velmi široká a zaměřuje se na tři základní oblasti – osoby, majetek a informace. Pro každou oblast, která je předmětem bezpečnostních zájmů organizace, je třeba formulovat samostatnou bezpečnostní politiku (viz. Obrázek 6). [1,2]



Obrázek 6: Pozice bezpečnostní politiky v organizaci

3 Informační bezpečnost

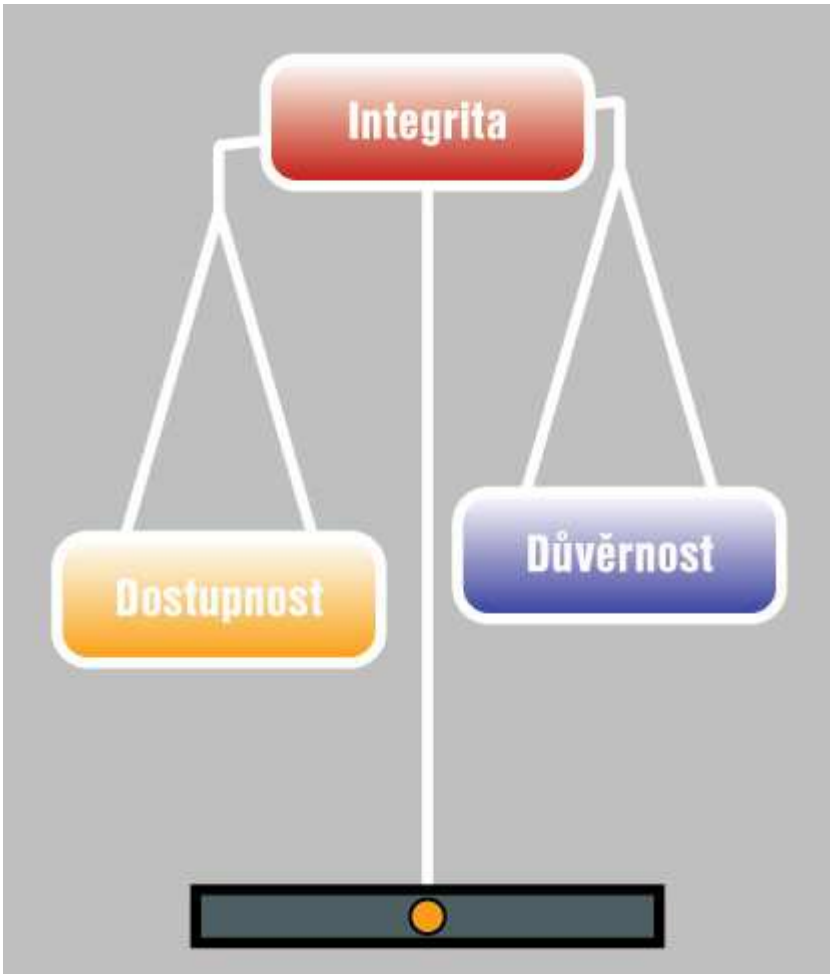
Bezpečnost osobních údajů a informací je z pohledu celkového zabezpečení organizace, v našem případě městského úřadu, dílčím problémem. Informace jsou nejcennější devizou každé organizace, a proto je nezbytné je co nejlépe zabezpečit v celém rozsahu jejich struktury. Nerozhoduje, zda se jedná o informace v elektronické nebo papírové podobě, umístěné v informačních systémech nebo mimo ně.

Informační bezpečnost je charakterizována jako zachování důvěrnosti, integrity a dostupnosti (Obrázek 7).

- **Důvěrnost -** znamená zajištění toho, aby informace byla dostupná pouze oprávněným osobám.
- **Integrita -** znamená zabezpečení správnosti a kompletnosti informací a metod zpracování.
- **Dostupnost** - znamená zajištění toho, aby informace a s nimi spojená aktiva byly přístupné pouze autorizovaným uživatelům podle jejich potřeby.

Informace je třeba chápat jako majetek a podle toho zajistit i jejich bezpečnost. Veřejná správa, na jejíž modernizaci a elektronizaci je kladen čím dál tím větší tlak, musí neodkladně zavést odpovídající bezpečnostní opatření.

Bezpečnost informačních systémů (dále IS) se často podceňuje, protože dokud nedojde k bezpečnostnímu incidentu, nepřináší vložené investice do zabezpečení žádné výsledky. V případě nedostatečného zajištění informační bezpečnosti může být ohrožena bezpečnost a hospodářské zájmy státu, soukromého sektoru i občanů a oslabit důvěryhodnost dané organizace. Škody a ztráty informací mohou vyvolat další práci a náklady, které by nevznikly, kdyby byla ochrana těchto informací dostatečná. Je třeba brát v úvahu, že informace a osobní údaje se vyskytují také v listinné podobě a přijmout tak účinná opatření k jejich ochraně. [12,19]



Obrázek 7: Převaha důvěrnosti nad dostupností se zajištěním integrity

Informační systém se skládá z:

Informační technologie – vstup, zpracování, uložení, přenos, prezentace dat

- Hardware (dále jen HW) – komponenty výpočetních systémů (CPU, HDD, RAM apod.), propojovací síťové prvky, kabely, zdroje apod.
- Software (dále jen SW) – operační systémy, aplikační programové vybavení apod.

Data – soubory a databáze, vstupní data, výstupní sestavy, výsledná data apod.

Lidé – uživatelé, obsluha, správci operačních systémů, databází, sítí apod. [14]

Při zajišťování bezpečnosti je nutné brát v úvahu všechny výše zmíněné hlediska. Bezpečnost IS je třeba brát jako proces, který nikdy nekončí. Pokud totiž budeme mít např. zavedený antivirový program do počítače, ale nebudeme ho aktualizovat, ztratí tento program svou funkci a význam.

3.1 Zabezpečení informací v objektu

Personální bezpečnost - jedná se především o preventivní ochranu informačních systémů z pohledu konkrétních událostí způsobených zaměstnanci. Musí být zajišťována jak prověřováním budoucích zaměstnanců instituce, tak opakujícími se prověrkami stávajících zaměstnanců. Velký význam má zejména v případě, že organizace zpracovává nebo jinak nakládá s utajovanými informacemi.

Režimová bezpečnost – určuje pravidla pro práci s informacemi, daty, komunikačními a počítačovými systémy. Je významným prvkem prevence. Zahrnuje systém práce s písemnostmi, systém ukládání datových médií, vymezení okruhu osob, které pracují s osobními údaji a daty, apod.

Nejdůležitějším dokumentem v rámci režimové bezpečnosti informací je Spisový řád. V tomto řádu by měly být určeny zásady oběhu dokumentů, systém jejich posuzování a schvalování, předávání, jejich kopírování, ukládání, uzamykání, poštovní přeprava a postup v případě ztráty. V oblasti režimové ochrany je nezbytné přijmout pravidla pro skartační činnost, užívání komunikačních či sdělovacích prostředků, jako užívání telefonů popřípadě faxu. Je nutné stanovit kdy a jak užívat rozmnožovacích prostředků (kopírek) a jaké osoby mohou s konkrétními prostředky pracovat.

Fyzická bezpečnost – jejím hlavním účelem je, zamezovat neoprávněnému a neautorizovanému přístupu k informacím a počítačovým systémům, vniknutí do prostor, kde se tyto informace nacházejí a předcházet poškození a narušení informací. Zahrnuje také kontrolu vstupu a vymezení přesného způsobu práce osob v oblastech, kde se informace nacházejí, zabezpečení kanceláří, místností, zařízení a kabeláže.

Bezpečnost technických prostředků (ochrana HW) – jedná se o praktické použití technických prostředků určených k ochraně informací nebo nakládání s nimi a určení pravidel jejich používání, kontroly a údržby. Např. zde patří zabezpečení míst, kde se nacházejí trezory s informacemi, identifikační karty, autentizační kalkulátory, záložní kopie dat, záložní zdroje elektrické energie v případě výpadku apod.

Všechny důležité spisy, listiny, finance, cenné předměty a další věci v hmotné podobě by se měly umisťovat např. do trezorů, aby byla zajištěna ochrana proti odcizení nebo proti zničení požárem (ohnivzdorná kartotéková skříň, EPS apod.).

Bezpečnost softwarových prostředků – jde o souhrn opatření, které ochrání programové vybavení před viry, zničením či poškozením, zabraňuje v přístupu nepovolaným

osobám do informačního systému, monitoruje činnost osob při práci s informačním systémem. Zejména zde patří logické bezpečnostní funkce, jako softwarové řízení přístupu za použití kryptografie, digitální podepisování, antivirové prostředky, ochranné nástroje v operačních systémech, ochrana paměti, ochrana souborů řízením přístupu, přístupové matice, přístupové seznamy a hesla, ochrana sítí apod. [9]

Data uvnitř počítače můžeme chránit několika způsoby:

- **Zálohováním** – obvykle se provádí v určitých časových intervalech kompletní zálohování všech dat a v mezidobí se provádí zálohování pouze těch dat, u kterých došlo od poslední zálohy ke změně..
- **Vytvářením a rušením uživatelských kont** – vytváří se proto, aby se zaměstnanec mohl připojit k síti, ale s předem nastavenými přístupovými právy. Při odchodu zaměstnance, ať už do jiného zaměstnání nebo do důchodu, by se měla tato konta naopak rušit.
- **Řízením manipulace s přenosnými médií** – jde o média využívaná pro přenos dat v organizaci. Řadíme mezi ně CD, DVD apod. Je potřeba stanovit, jak s daty nakládat, tzn., zda lze tato data ukládat na přenosná média a jestli je lze volně vynášet z organizace.
- **Šifrováním dat –** šifrování dat by se mělo provádět pokud jsou data přenášena po nechráněné cestě. [2,8]

3.2 Informační kriminalita

Počítačovou kriminalitu je třeba chápat jako páchání trestné činnosti, v níž figuruje počítač jako souhrn technického a programového vybavení (nebo pouze některá z jeho komponent) včetně dat, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět této trestné činnosti nebo jako nástroj trestné činnosti. Počítačová kriminalita se stala fenoménem konce dvacátého století a i dnes následuje její prudký rozvoj. Souvisí to především se značným rozšířením výpočetní techniky v ekonomice, v prudkém růstu jejího užívání v domácnostech a zejména v rozvoji počítačových sítí a zvláště internetu.

V poslední době se používá spíše pojem informační kriminalita, zvláště pokud chceme zdůraznit, že trestný čin má vztah k datům, resp. uloženým informacím, nebo obecněji

k informačním technologiím. V zahraničí se také často používá pojem ”kyberzločin” (”Cyber-Crime”) nebo ”high-tech” zločin.

Počítačové sítě jsou v dnešním světě základním komunikačním prostředkem v rámci fungování organizace. Proto je nezbytné je chránit před hrozbami, které by způsobily jejich napadení. [4]

Informační kriminalitu dělíme na:

Porušování autorského práva tzv. softwarové pirátství

Softwarovým pirátstvím se myslí všechny útoky na práva autora a další práva k počítačovým programům. K porušování autorských práv dochází většinou užíváním programu na jednom počítači případně více počítačích než bylo ve smlouvě dohodnuto, zasahováním do programu, prováděním jeho změn a úprav nebo šířením tohoto programu jiným osobám (nejčastěji okopírováním, ale také výrobou a prodejem plagiátů).

Poškození a zneužití záznamu na nosiči informací

Poškození a zneužití nosiče informací je pokládáno za jeden z nejnebezpečnějších útoků na jakákoliv data. Hlavní nebezpečí je v tom, že pachatel může spáchat tento zločin beze stop a bez odhalení správcem dat, což je zásadní bezpečnostní riziko. Může docházet k útokům na data klientských databází různých organizací jako nástroj konkurenčního boje, ke kopírování bezpečnostních, vědeckovýzkumných a podobně citlivých dat.

- **Útok z vnějšku subjektu**

Tímto způsobem útoku se myslí tzv. hacking, neboli neoprávněné získání přístupu k datům. Jde o narušení ochrany počítače pachatelem, který není u počítače fyzicky přítomen a většinou se nachází daleko od cíle útoku. Podmínkou je připojení výpočetní techniky obvykle po telefonní nebo jiné lince. Jedná se např. o virovou nákazu, průnik do sítě, odposlech provozu zařízení uvnitř organizace z vnějšku, přístup k nezabezpečeným komunikačním kanálům apod.

Důvody útoku:

- neoprávněné získání a užití informací
- zničení, poškození nebo učinění informací neupotřebitelnými – destrukce, poškození nebo upravení dat

- zásah do technického nebo programového vybavení počítače

- **Útok zevnitř subjektu**

Tyto útoky pak můžeme dělit na útoky úmyslné (např. vnější útočníci, jako špionáž, terorismus, kriminální živly, vnitřní útočníci jako propuštěný, rozzlobený, vydíraný, chamtivý zaměstnanec) a neúmyslné (nedostatečná kvalifikace či proškolení). Útok od zaměstnance může být závažný, zvlášť pokud zaměstnanec disponuje důvěrnými informacemi.

- **Útoky kombinované**

  Jedná se o útok z vnějšku i zevnitř.

Ostatní informační trestná činnost

Patří zde trestné činy, které výpočetní techniku využívají jako prostředek k páchání trestných činů, nikoliv jako přímý objekt zájmu pachatele. Jedná se zejména o využívání internetu ke grafické a verbální kriminalitě – zveřejňování návodů k násilné trestné činnosti (návody na výrobu výbušnin, zbraní apod.), k páchání mravnostní kriminality (dětská pornografie) nebo verbální kriminality (extremismus, vyhrožování), k praní špinavých peněz a jiným formám finanční kriminality apod. [16,17]

3.3 Bezpečnostní politika informačního systému

Politika bezpečnosti je podřízena celkové bezpečnostní politice organizace (viz. obrázek 6) a té je podřízena politika informační bezpečnosti. Bezpečnostní politika organizace tvoří jeden ze základních pilířů, na kterém stojí systém řízení informační bezpečnosti. Bezpečnostní politika informačních systémů (dále jen BPIS) a informačních technologií (dále jen IT) definuje základní bezpečnostní požadavky a nařízení, které mají za cíl zajistit ochranu a bezpečnost informací v organizaci. Reflektuje závěry získané z analýzy rizik IS a definuje mechanismy zajišťující efektivní řízení informační bezpečnosti. Je podkladem pro budování nižších a specifických stupňů bezpečnostní dokumentace.

Mezi hlavní přínosy definované BPIS patří:

- přináší do organizace jasně formulované základní principy řízení informační bezpečnosti,
- všichni zaměstnanci musí znát své základní odpovědnosti a povinnosti při práci s informacemi,

- definuje základní požadavky na chování vnějších subjektů v prostředí informačního systému organizace,
- zvyšuje kredit organizace u spolupracujících subjektů,
- je vypracována na základě současných nejlepších norem a standardů používaných v oblasti bezpečnosti.

Problémem zabezpečení vlastního informačního systému se zabývá pravděpodobně naprostá většina podniků rozličného zaměření a velikosti. Řešením informační bezpečnosti v organizaci bývá pověřen management informační bezpečnosti. [3]

Typy BPIS:

Promiskuitní – neomezující, zaručuje minimální nebo nulovou úroveň bezpečnosti IS.

Liberální – neopatrná, explicitní zákazy, vhodné řešení pro IS se slabými hrozbami a nízkým ohodnocením informací.

Racionální – opatrná, explicitní povolení, zaručuje vyšší stupeň bezpečnosti, vyžaduje provedení klasifikace objektů a subjektů podle jejich citlivosti a povinné řízení přístupu k nim.

Paranoidní – vše zakazující, zaručuje vysoký stupeň bezpečnosti za cenu izolace IS s minimem možných přístupů.

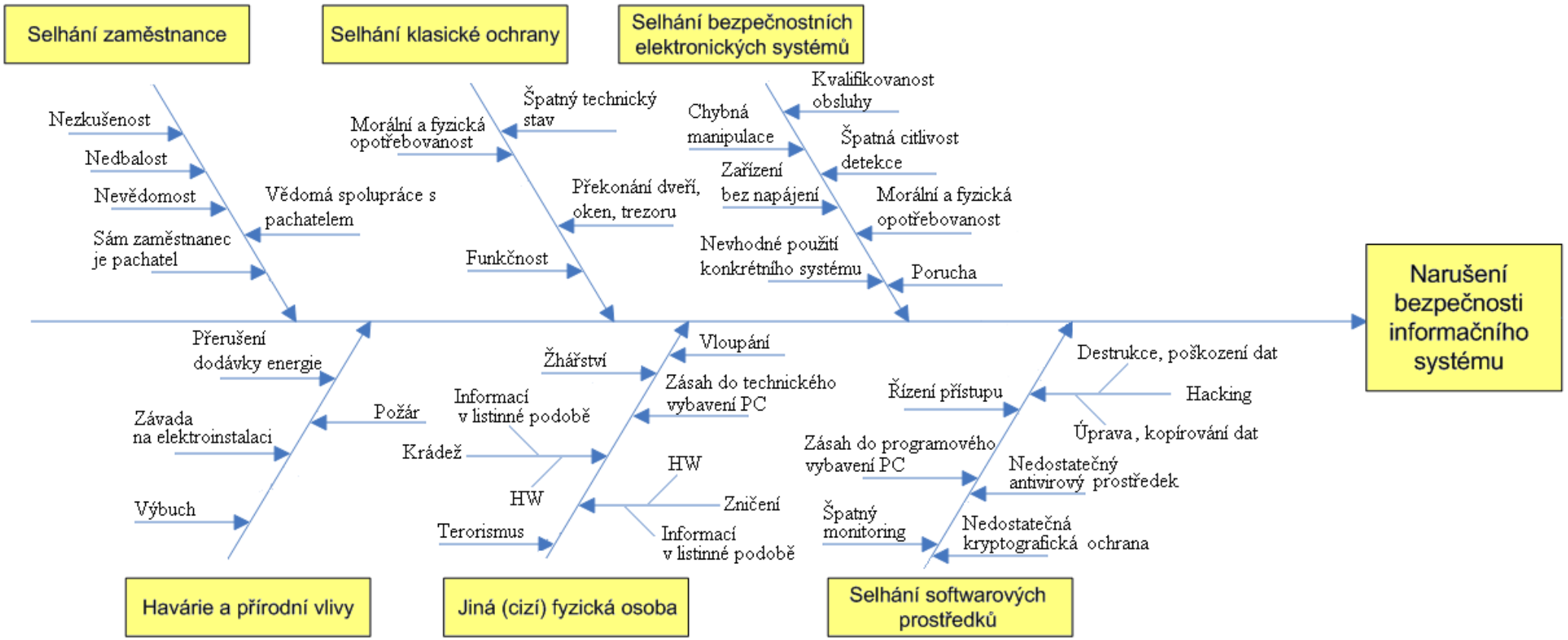
4 Bezpečnostní analýza objektu městského úřadu

Ochrana informací a osobních údajů by měla být řešena komplexně, kde kromě zabezpečení informací podniku patří i ochrana majetku a zaměstnanců, a proto se ve své bakalářské práci zabývám ochranou informací komplexně.

Aby byla bezpečnostní rizika posouzena objektivně je nutné provést analýzu těchto rizik. Analýzu lze charakterizovat jako metodu poznání, kdy postupujeme od obecného ke konkrétnímu. Zkoumá předměty, jevy, informace a skutečnosti dotýkající se přímo či nepřímo bezpečnosti organizace, s cílem přispět k nalezení přiměřených bezpečnostních prostředků a opatření, která jsou vhodná k účinnému a adekvátnímu řešení bezpečnostního problému organizace. Ve své bakalářské práci jsem zvolila analýzu k identifikaci pomocí Ishikawova diagramu (tzv. rybí kostra) a poté použiji metodu FTA (Fault Tree Analysis – analýza stromem poruch). Zjištěná rizika budu dále hodnotit metodou FMEA (Failure Modes And Effects Analysis. [18]

4.1 Modelování rizik Ishikawovým diagramem

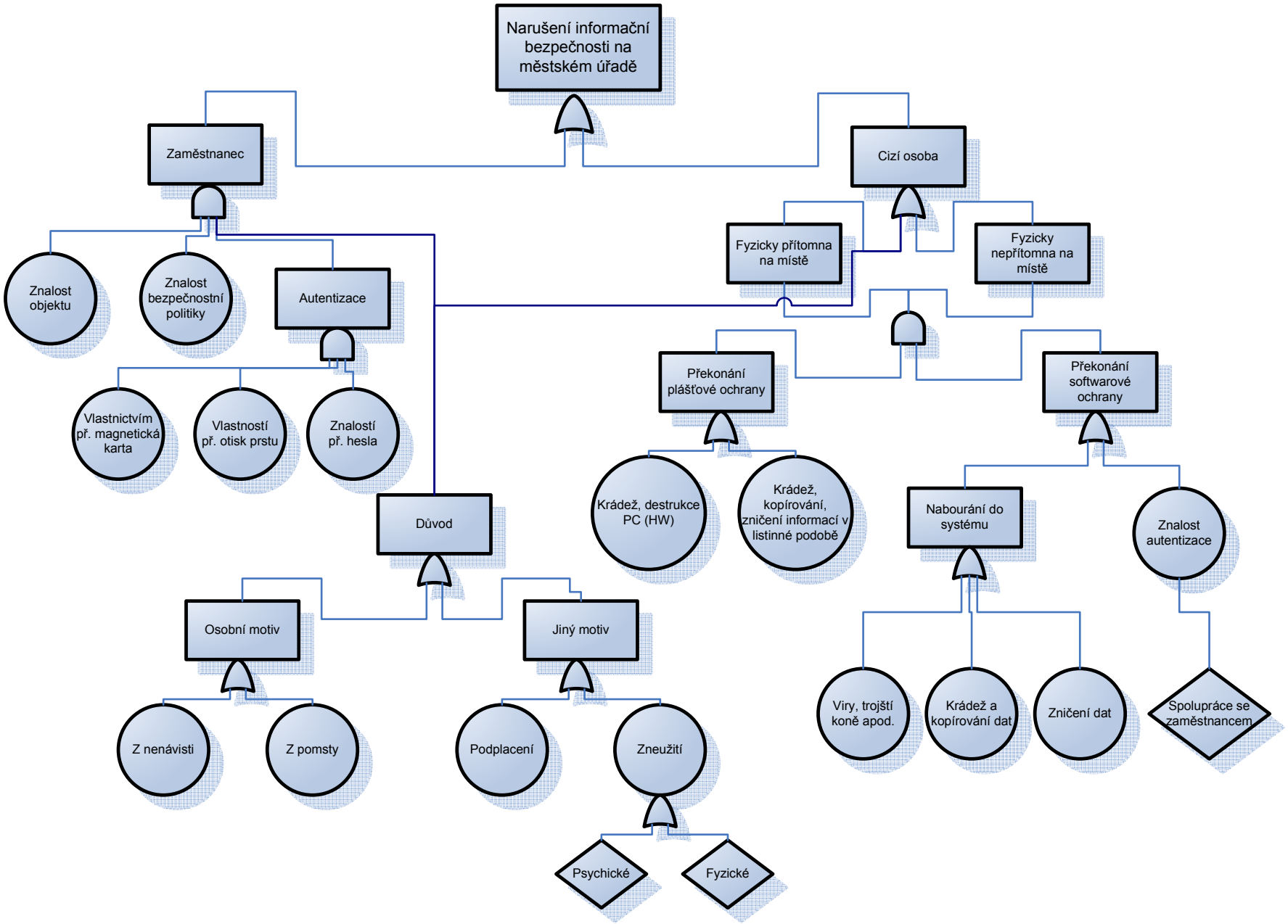
Ishikawův diagram, známý též pod názvem diagram příčin a důsledků nebo rybí kost, slouží k systematickému popisu všech možných příčin, které je možno definovat u určitého jevu. Umožňuje jednoduše znázornit konkrétní analyzovaný problém z hlediska jeho příčin. Rizika, která mohou ohrozit bezpečnost informačního systému jsou znázorněna na Obrázku 8.



Obrázek 8: Ishikawův diagram

4.2 Modelování rizik metodou FTA

Metoda FTA, strom poruch je deduktivní metoda, která identifikuje jednotlivá rizika a určuje příčiny těchto rizik. Je založena na Booleovské algebře (hradla „a“, „nebo“) při vyhledávání možných důsledků. Rizika narušení informačního systému na městském úřadě je znázorněno na Obrázku 9.



Obrázek 9: Grafické znázornění modelování rizik pomocí FTA

4.3 Výpočet analýzy FMEA

Aby byla bezpečnostní rizika posouzena objektivně, musíme provést jejich analýzu, která umožní odhalení rizik a následný návrh vhodných opatření. K tomuto jsem si vybrala metodu FMEA (Failure Modes And Effect Analysis). Identifikuje jednoduché poruchy a jejich následky. Tato analýza se řadí mezi analytické metody a systematicky se z ní zjišťují následky poruchových stavů jednotlivých dílčích celků. Lze ji použít jak pro identifikaci nebezpečí, tak pro odhad pravděpodobnosti jeho vzniku a kritické posouzení možných následků. Charakterizuje a hodnotově vyjadřuje systémovou závislost mezi příčinou a následkem. Stěžejní rizika daného subsystému se hodnotí pomocí tří indexů. [18]

První index je označen písmenem „**P**“ – pravděpodobnost vzniku a existence rizika. Obsahuje pět stupňů které dokumentují pravděpodobnost vzniku dané události nebo rizika. Jednotlivé stupně i s názvoslovím jsou uvedeny v Tabulce 1.

Tabulka 1: Stupně pravděpodobnosti vzniku rizika

P	Pravděpodobnost vzniku a existence rizika
1	nahodilá
2	nepravděpodobná
3	pravděpodobná
4	velmi pravděpodobná
5	trvalá hrozba

Druhý index je označen písmenem „**N**“ – závažnost následků. Taktéž obsahuje pět stupňů určujících závažnost rizika v dopadu na zdraví osob, životní prostředí, finanční, materiální i důvěryhodnost vůči organizaci. Stupně jsou uvedeny v Tabulce 2.

Tabulka 2: Stupně závažnosti následků

N	Závažnost následků
1	malá škoda
2	větší škoda
3	vyšší škoda
4	vysoká škoda

5	velmi vysoká škoda

Třetí index je označen písmenem „**H**“ – odhalitelnost rizika. Rovněž zahrnuje pět stupňů stanovujících, jak rychle a snadno dané riziko či událost zjistíme. Stupně jsou uvedeny v Tabulce 3.

Tabulka 3: Stupně odhalitelnosti rizika

H	**Odhalitelnost rizika**
1	velmi snadno odhalitelné riziko
2	snadno odhalitelné riziko
3	odhalitelné riziko
4	nesnadno odhalitelné riziko
5	neodhalitelné riziko

Následná míra rizika se stanoví jako součin indexů P, N a H, jak je uvedeno v rovnici 1.

$$R = P \cdot N \cdot H \tag{1}$$

Kde „**R**“ je míra rizika. Dělí se do pěti kategorií jak je uvedeno v Tabulce 4.

Tabulka 4: Kategorie míry výsledného rizika

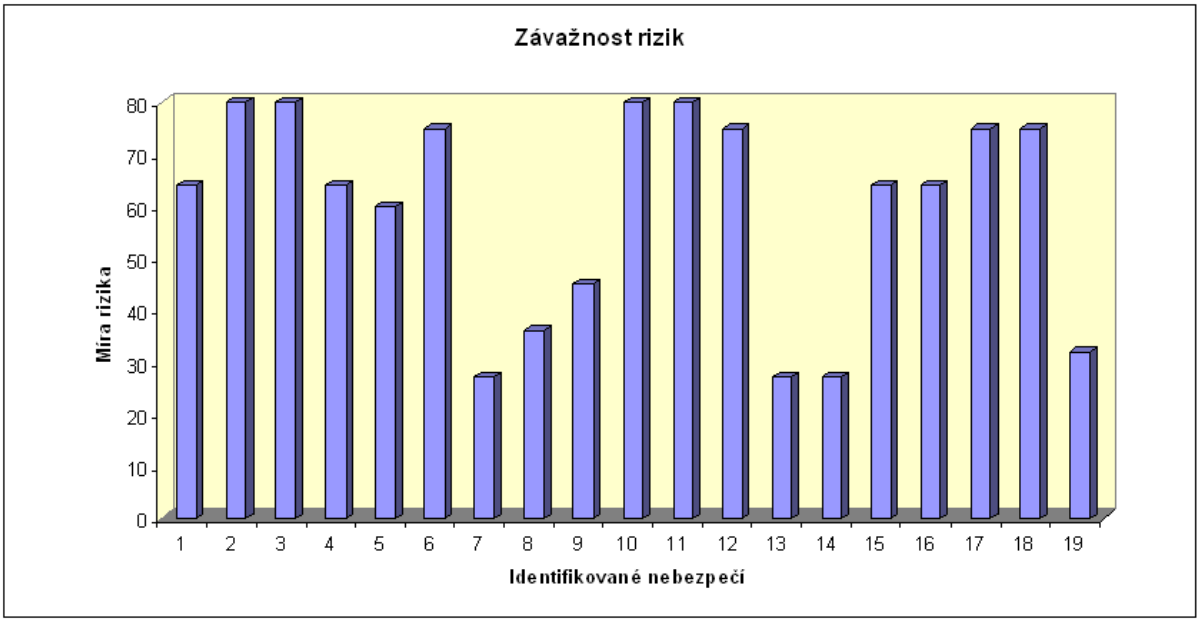
R	**Míra rizika**
0 – 3	bezvýznamné riziko
4 – 10	akceptovatelné riziko
11 – 50	mírné riziko
51 – 100	nežádoucí riziko
101 – 125	nepřijatelné riziko

Pomocí těchto hodnot se stanoví míra rizika „R“ v intervalu (0,125>. Hodnoty jednotlivých indexů v tabulkách jsou lehce nadsazené. Při konečném vyhodnocení míry rizika jsem vypočetla tzv. míru tolerance, která určuje hranici rizika jako přijatelné nebo

nepřijatelné. Výsledkem této analýzy je grafická podoba rizik, která názorně ukazuje závažnost jednotlivých rizik podle toho, jestli překračují stanovenou míru tolerance či nikoliv. Jednotlivá rizika vypočtená touto metodou, jsou uvedena v Tabulce 5 a graficky vyjádřená na Obrázku 10.

Tabulka 5: Jednotlivá rizika vypočtená metodou FMEA

Výčet jednotlivých rizik		P	N	H	R
1	Vniknutí do budovy	4	4	4	64
2	Překonání vstupních dveří	5	4	4	80
3	Neoprávněný vstup do neveřejných prostor	5	4	4	80
4	Překonání oken	4	4	4	64
5	Vniknutí na střechu	3	5	4	60
6	Požár nebo výbuch v budově	5	5	3	75
7	Výpadek elektrického proudu	3	3	3	27
8	Porucha	4	3	3	36
9	Špatná citlivost detekce	3	5	3	45
10	Zaměstnanec je pachatelem	5	4	4	80
11	Vědomá spolupráce zaměstnance s pachatelem	5	4	4	80
12	Nezkušenost, nedbalost, nevědomost zaměstnance	5	5	3	75
13	Krádež informací v listinné podobě	3	3	3	27
14	Poškození, zničení informací v listinné podobě	3	3	3	27
15	Krádež počítačové techniky a dat z počítače	4	4	4	64
16	Poškození, zničení počítačové techniky a dat v počítači	4	4	4	64
17	Nabourání se do sítě	5	5	3	75
18	Viry, trojští koně apod.	5	5	3	75
19	Odcizení věcí z trezoru	4	3	3	36



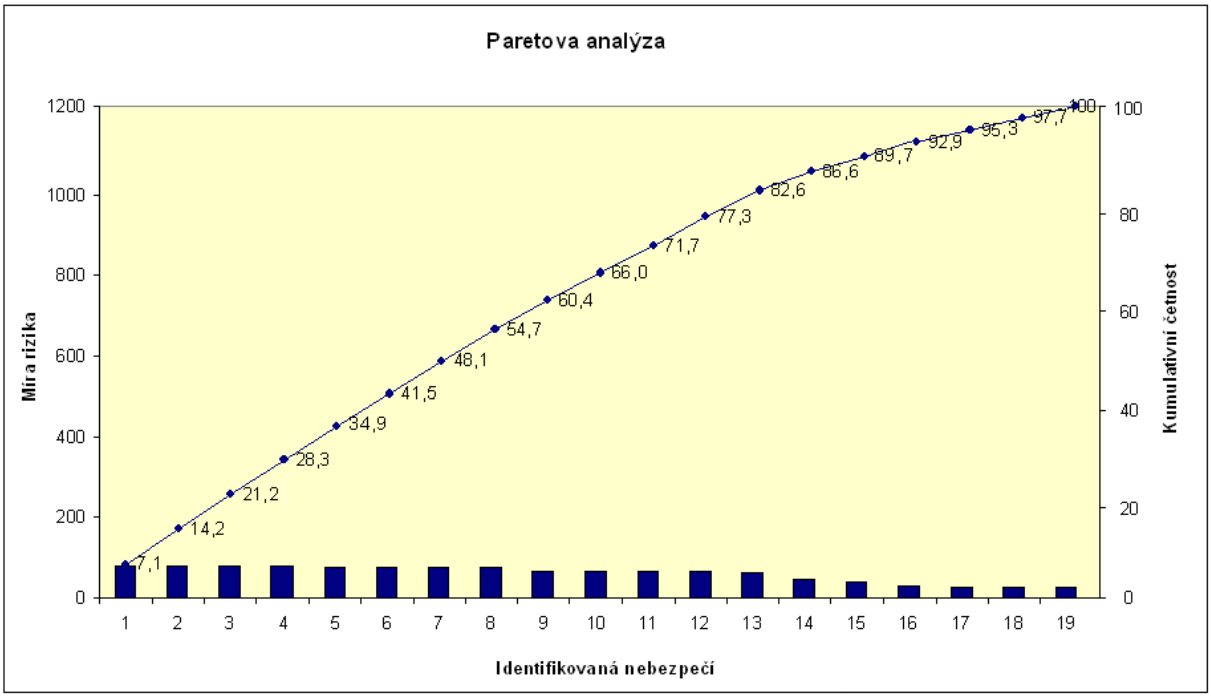
Obrázek 10: Graf závažnosti rizik metody FMEA

Ke správnému vyhodnocení analýzy byla použita Paretova analýza a Lorenzova křivka kumulativních četností, pomocí kterých byl sestaven graf uvedený na Obrázku 11. V oblasti bezpečnosti vychází analýza z předpokladu, že za 80% problémů stojí 20% příčin, nebo naopak 20% úsilí vloženého do oblasti bezpečnosti přinese 80% žádoucího efektu. Ukazuje, kam by se měla zaměřit pozornost a úsilí. Kvůli přehlednosti jsem sestavila Tabulku 6, ve které jsou vypočtená rizika metody FMEA seřazena od nejzávažnějších. V prvním sloupci je uvedeno pořadové číslo rizika od nejzávažnějšího, ve druhém sloupci číslo rizika podle Tabulky 5, ve třetím sloupci jsou uvedená rizika vyjádřena procenty, ve čtvrtém sloupci je postupně sečteno procentuální riziko jednotlivých nebezpečí a do stanoveného limitu 80% jsou rizika označena červeně.

Tabulka 6: Jednotlivá rizika vpočtená metodou FMEA seřazená podle závažnosti

Pořadové číslo	Číslo rizika podle FMEA	Míra rizika	Četnost (%)	K. četnost
1	2	80	7,1	7,1
2	3	80	7,1	14,2
3	10	80	7,1	21,2
4	11	80	7,1	28,3

5	6	75	6,6	34,9
6	12	75	6,6	41,5
7	17	75	6,6	48,1
8	18	75	6,6	54,7
9	1	64	5,6	60,4
10	4	64	5,6	66,0
11	15	64	5,6	71,7
12	16	64	5,6	77,3
13	5	60	5,3	82,6
14	9	45	4,0	86,6
15	8	36	3,2	89,7
16	19	36	3,2	92,9
17	7	27	2,4	95,3
18	13	27	2,4	97,7
19	14	27	2,4	100
celkem		1130	100	



Obrázek 11: Grafický výstup rizik podle tabulky 6

Provedenou analýzou s použitím Paretova principu a Lorenzovy křivky byla jako nejzávažnější zjištěna tato rizika:

- vniknutí do budovy,
- překonání vstupních dveří,
- neoprávněný vstup do neveřejných prostor,
- překonání oken,
- požár nebo výbuch v budově,
- zaměstnanec je pachatel,
- vědomá spolupráce zaměstnance s pachatelem,
- nezkušenost, nedbalost, nevědomost zaměstnance,
- krádež počítačové techniky a dat z počítače,
- poškození, zničení počítačové techniky a dat v počítači,
- nabourání se do sítě, viry, trojští koně.

5 Osobní údaje na městské úřadě

Městský úřad tvoří starosta, místostarostové, tajemník (vedení města) a zaměstnanci města do něj zařazení. Člení se na odbory a útvary, které jsou jeho základní organizační jednotkou. V čele odboru stojí vedoucí odboru. Odbory se dále vnitřně člení na nižší organizační stupně, kterými jsou oddělení. Oddělení zajišťují ucelenou agendu a v jejich čele stojí vedoucí oddělení.

Městský úřad se člení na tyto odbory:

- organizační odbor
    - kancelář tajemníka
    - oddělení hospodářské správy a krizového řízení
- odbor informatiky
- finanční odbor
    - oddělení financí a rozpočtu
    - oddělení účetnictví
- odbor obecního podnikání
    - oddělení investiční
    - oddělení komunálního hospodářství
    - oddělení rozvoje města
- majetkoprávní odbor
    - oddělení majetkové
    - oddělení právní
- odbor vnitřních věcí
    - oddělení evidence obyvatel, občanských průkazů a cestovních dokladů
    - oddělení matrik
- odbor správních deliktů
- odbor dopravy a silničního hospodářství
    - oddělení evidence řidičských průkazů a motorových vozidel
    - oddělení silničního hospodářství
    - oddělení správní
- odbor školství, kultury, mládeže a tělovýchovy
    - oddělení kultury sportu a volného času

    - oddělení školství
- odbor územního plánování, stavebního řádu a památkové péče
    - oddělení stavební úřad
    - oddělení úřad územního plánování
- odbor životního prostředí
    - oddělení ochrany přírody, lesnictví a myslivosti
    - oddělení odpadů, ochrany ovzduší a zemědělského půdního fondu
    - oddělení vodního hospodářství
- odbor sociálních věcí
    - oddělení dávek hmotné nouze
    - oddělení sociální práce
    - oddělení dávek pro zdravotně postižené a seniory
    - oddělení sociálně právní ochrany dětí
    - oddělení bytové
- odbor obecní živnostenský úřad
    - oddělení správní
    - oddělení registrační
    - oddělení kontroly
    - informační centrum
- kontrolní odbor

Největší množství osobních údajů na městském úřadě zpracovává odbor vnitřních věcí. Tento odbor se skládá z oddělení evidence obyvatel, občanských průkazů, cestovních dokladů a oddělení matriky.

Oddělení matriky:

- plní úkoly stanovené na úseku matrik jako matriční úřad,
- plní úkoly stanovené na úseku matrik jako úřad obce s rozšířenou působností,
- plní úkoly stanovené na úseku státního občanství,
- plní úkoly na úseku identifikace osob podle zák. č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu ve znění pozdějších předpisů,
- přenáší metodiku KÚ MS kraje na úseku vidimace a legalizace na ověřující úředníky a koordinuje jednotnost postupu na tomto úseku na MÚ,

- zajišťuje provozování částečného kontaktního místa pro případ zastupování Czech POINT pro ověřené výstupy z rejstříku trestu pro potřeby občanů,
- provádí identifikace osob (dle zákona o boji proti legalizaci výnosů z trestné činnosti).

Oddělení evidence obyvatel, občanských průkazů a cestovních dokladů:

- plní úkoly stanovené na úseku evidence obyvatel jako ohlašovna,
- plní úkoly stanovené na úseku evidence obyvatel jako úřad obce s rozšířenou působností,
- plní úkoly stanovené na úseku sčítání lidu, domů a bytů,
- plní úkoly stanovené na úseku občanských průkazů,
- plní úkoly stanovené na úseku cestovních dokladů.

Každý úředník těchto oddělení pracuje s osobními údaji, jejichž nejčastějšími druhy jsou jméno, příjmení, rodné příjmení, rodné číslo, datum narození, místo narození, adresa trvalého pobytu, adresa přechodného pobytu, fotografie, zbavení nebo omezení způsobilosti k právním úkonům, pohlaví, rodinný stav apod. Osobní údaje se zpracovávají v listinné a elektronické podobě. Elektronicky jsou zpracovávány v informačních systémech MV ČR, čímž se MV ČR stává správcem osobních údajů. Požadavky na ochranu osobních údajů nejsou stanoveny obecně závazným právním předpisem, vychází se pouze ze zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů. [20]

5.1 Návrh zabezpečení objektu městského úřadu

Na základě provedených analýz FTA, FMEA byla zjištěna nejzávažnější rizika z pohledu ochrany osobních údajů a informací. Pro minimalizaci vyhodnocených nejzávažnějších rizik jsem na základě teoretických znalostí navrhla opatření uvedená v Tabulce 7. [15]

Tabulka 7: Návrh opatření pro minimalizaci rizik

Nejzávažnější vyhodnocená rizika	Opatření k minimalizaci rizik
Vniknutí do budovy	Všechny dveře zabezpečit bezpečnostními zámky. Dále také přijmout bezpečnostní opatření při napojení na velkoprůměrovou kanalizaci, propustní a ventilační šachty, kabelové šachty, kanály a šachty teplovodů, šachty s výtahy, systém vzduchotechniky apod.
Překonání vstupních dveří	Všechny dveře zabezpečit bezpečnostními zámky. U hlavních vstupních dveří zajistit fyzickou ochranu.
Neoprávněný vstup do neveřejných prostor	Zabezpečit prostory kamerovým systémem a fyzickou kontrolou. Vybavit neveřejné prostory bezpečnostními zámky.
Překonání oken	Všechna okna objektu v prvním nadzemním podlaží (1.NP) zabezpečit mřížemi, v ostatních patrech navrhuji bezpečnostní folie.
Požár nebo výbuch v budově	Budovu zabezpečit elektrickou požární signalizací, hasícími přístroji. Místnosti, kde se nacházejí informace a osobní údaje vybavit ohnivzdornými trezory, skříňkami, stabilním hasícím zařízením apod. Vymezit prostor pro kuřáky. Dále by pracoviště mělo být vybaveno pokyny při vypuknutí požáru nebo požárním řádem na viditelném místě.
Zaměstnanec je pachatelem	Prověřování přijímaných zaměstnanců, motivací zaměstnanců, formy odměn a benefitů, příjemným pracovním prostředí. Vyvolat v zaměstnanci sounáležitost a loajalitu s organizací. Vést záznam kdo, kdy a z jakého důvodu pracoval s osobními údaji.
Vědomá spolupráce zaměstnance s pachatelem	Prověřování přijímaných zaměstnanců, motivací zaměstnanců, formy odměn a benefitů, příjemným pracovním prostředí.Vyvolat v zaměstnanci sounáležitost a loajalitu s organizací. Vést záznam kdo, kdy a z jakého důvodu pracoval s osobními údaji.
Nezkušenost, nedbalost, nevědomost zaměstnance	Výcvik a školení zaměstnanců. Pravidelné přestávky pro zaměstnance.
Krádež počítačové techniky a dat z počítače	Počítačovou techniku, v případě nepřítomnosti uživatele, uzamknout v bezpečnostní skříňce. Vytvořit uživatelské konta. Místnosti s počítačovou technikou vybavit elektrickou zabezpečovací signalizací. Zajistit ochranu proti nabourání se do sítě. Omezit počet pokusů na udání hesla a v případě překročení limitu zakázat na nějakou dobu přístup do systému. Šifrovat data.
Poškození, zničení počítačové techniky a dat v počítači	Zajistit zálohování dat v počítači. Vytvořit uživatelské konta. Použít šifrovače pro ochranu informací přenášených po nechráněných cestách. Zajistit záložní zdroje elektrické energie při výpadku el. proudu. Zajistit ochranu proti nabourání se do sítě. Místnosti s počítačovou technikou vybavit EPS. V případě nepřítomnosti uživatele uzamknout počítačovou techniku v bezpečnostní skříňce.

Nabourání se do sítě	Pracovníci by si neměli navzájem sdělovat přihlašovací jména a hesla, ani si je nikam psát. Hesla by neměla být lehce odhadnutelná, tzn. nesmí odpovídat jménům zaměstnanců či jejich rodinných příslušníků, datu narození apod. Zaměstnanci by dále neměli využívat internet k navštěvování nebezpečných stránek či stahovat a odesílat nebezpečné přílohy, samospustitelné aplikace apod. Rizikovému chování při používání internetu může předcházet správně nastavená bariéra Firewall nebo Proxyserver. Pro další zvýšení zabezpečení lze využívat přístupové karty, omezení práv přístupu uživatelů k datům podle jejich skutečných potřeb a stupně důležitosti dat, nastavení práv uživatelů komunikujících prostřednictvím internetu, protivirovou kontrolu veškeré komunikace směřující dovnitř i ven z vnitřní sítě a podobně. Omezit počet pokusů na udání hesla a v případě překročení limitu zakázat na nějakou dobu přístup do systému. Zajistit ochranu pomocí speciálních programů, které jsou k tomu určeny, tzv. firewally.
Viry, trojští koně apod.	Instalace antivirových prostředků a zajištění jejich aktualizací.

Závěr

Bakalářskou prací jsem zpracovala přehled problematiky při ochraně osobních údajů a informací na městském úřadě. Hlavním cílem této práce bylo analyzovat a zhodnotit bezpečnostní rizika při ochraně osobních údajů a informací a následně se pokusit navrhnout možná opatření pro jejich zmírnění.

Pro tento typ objektu jsem vypracovala bezpečnostní analýzu, ve které jsem se zaměřila na bezpečnost osobních údajů a informací. V analýze jsem použila několik metod. Pro identifikaci a posouzení rizik z hlediska příčin jsem využila diagram příčin a důsledku (tzv. rybí kost nebo ishikawův diagram) a metodu FTA. Tyto metody se jeví jako výhodné pouze pro stanovení možných příčin vzniku mimořádné události, ale neřeší jednotlivá rizika z hlediska jejich závažnosti pro objekt. Těmito metodami jsem provedla pouhou identifikaci možných rizik, které jsem analyzovala metodou FMEA. FMEA charakterizuje a hodnotově vyjadřuje systémovou závislost mezi příčinou a následkem.

Návrh opatření k minimalizaci nejzávažnějších rizik jsou uvedena v kapitole 5.1.

Seznam použité literatury

Literární zdroje:

[1] ADAMEC, V., ŠENOVSKÝ, M., *Základy krizového managementu*, Edice SPBI spektrum 28., 2. vyd. Ostrava 2004. 102 s. ISBN 80-86634-44-2.

[2] BRABEC, František, et al. *Bezpečnost pro firmu, úřad, občana.* Praha: Public History, 2001. 400 s. ISBN 80-86445-04-06.

[3] FRYŠAR, Miroslav, et al. *Bezpečnost pro manažery, podnikatele a politiky*. 1. vyd. Praha: Public History 2006. 176 s. ISBN 80-86445-22-4.

[4] JIROVSKÝ, Václav. *Kybernetická kriminalita*.[s.1.]: Grada, 2007. 288s. ISBN 978-80-247-1561-2.

[5] MATOUŠKOVÁ, M., HEJLÍK, L. *Osobní údaje a jejich ochrana.* 2. vyd. Praha: ASPI, Wolters Kluwer, 2008, 468 s. ISBN 978-80-7357-322-5

[6] ŠČUREK, Radomír. *Základní právní normy upravující ochranu objektu*. Ostrava : [s.n.], 2007. 37 s.

[7] ŠČUREK, Radomír, HOLUBOVÁ, Věra. *Ochrana objektu : Transport peněz, cenin a eskorta osob*. Ostrava : [s.n.], 2008. 113 s.

[8] ŠENOVSKÝ, Pavel. *Bezpečnostní informatika II*. 1. vyd. Ostrava : Sdružení požárního a bezpečnostního inženýrství, 2005. 37 s. ISBN 80-86634-61-2.

[9] ŠENOVSKÝ, Pavel. *Počítače a ochrana dat*. Ostrava : Sdružení požárního a bezpečnostního inženýrství, 2006. 47 s.

[10] UHLÁŘ, Jan. *Technická ochrana objektů : Mechanické zábranné systémy II*. 1. vyd. Praha : PA ČR, 2004. 178 s. ISBN 80-7251-172-6.

[11] UHLÁŘ, Jan. *Technická ochrana objektů : Elektrické zabezpečovací systémy*. 1. vyd. Praha : PA ČR, 2001. 205 s. ISBN 80-7251-076-2.

[12] Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.

Internetové zdroje:

[13] *ALFA secure s.r.o. : Perimetrická ochrana objektů* [online]. 2005 [cit. 2009-04-08]. Dostupný z WWW: <http://www.alfasecure.cz/fotogalerie-instalaci~1.html>.

[14] ČANČÍK, Jan. Bezpečnost informací se netýká jen IT firem. *Časopis IT □ystéme* [online]. 2008 [cit. 2009-04-08]. Dostupný z WWW: <http://www.systemonline.cz/it-security/bezpecnost-informaci-se-netyka-jen-it-firem-1.htm>.

[15] *Informační systémy veřejné správy : Bezpečnost IS* [online]. 2002 [cit. 2009-04-08]. Dostupný z WWW: <www.ISVS.CZ.>.

[16] *Ministerstvo vnitra České republiky* [online]. [cit. 2009-04-08]. Dostupný z WWW: <http://www.mvcr.cz/>.

[17] *Policie České republiky* [online]. [cit. 2009-04-08]. Dostupný z WWW: <http://www.policie.cz/>.

[18] *Přehled metodik pro analýzu rizik.* [online]. [cit. 3. 4. 2008]. Dostupné z: <http://www.krizove-rizeni.cz/index_soubory/dokumenty/anal.htm>

[19] *Úřad pro ochranu osobních údajů* [online]. 2000 , 17.04.2009 [cit. 2009-03-18]. Dostupný z WWW: <http://www.uoou.cz/>.

[20] VELIČKOVÁ , Dagmar. *Městský úřad Nového Jičína : Osobní údaje* [online]. 2006 , 14.1.2007 [cit. 2009-04-08]. Dostupný z WWW: <http://www.novy-jicin.cz/osobni-udaje/osobni-udaje.html>.

Seznam zkratek

č.	číslo
FMEA	analýza příčin poruch a jejich následků
FTA	strom poruch
KÚ MS kraje	Krajský úřad moravskoslezského kraje
MV ČR	Ministerstvo vnitra České republiky
např.	například
PIR čidlo	pasivní infračervené čidlo
tzn.	to znamená
tzv.	tak zvaně